The Future of Privacy Lies in Forgetting the Past

Jacquelyn Burkell*

What is the future of privacy? The easy and widespread response, that ‘privacy is dead’¹, is as overdone as it is unhelpful. The statement, of course, is no more true now than it would have been when Warren and Brandeis, in 1890, raised concerns about the impact of photography and the newspaper enterprise on privacy, remarking that these had ‘invaded the sacred precincts of private and domestic life’². Despite their very real and well-articulated concerns, we still have photography, we still have newspapers, and we still have privacy.

Warren and Brandeis did not embark on the project of ‘rolling back’ technology to return privacy to an earlier and possibly preferable state. Instead, they focused on protecting privacy, and particularly the instrumental value of privacy, in the context of technological and social changes. Today, we are faced with an explosion of new technologies and new information practices that raise unfamiliar privacy issues and heighten old privacy concerns. It is undeniable that these changes will influence the future of privacy – and it is equally undeniable that the nature of our future privacy will be determined by our collective response. What I would like to do here is to focus on three issues that I think are of particular, and indeed increasing, relevance to privacy – and to highlight a social, legal, and policy response that is perhaps best positioned to redress the negative privacy consequences that could arise.

The first, and perhaps most prominent, seismic change in the privacy landscape is the fundamental alteration of the nature and amount of personal information being produced, collected, and stored online. The most obvious source is social media profiles, which offer a continuing and accumulating record of lives lived: important dates, relationships, events, arguments, opinions, purchases, preferences, and plans are recorded in the form of images, messages, links, likes, and comments. We actively provide information when we sign up for, or log in to, various online services. Less obvious are the times when information is *captured*, rather than *offered*. Changing technologies have breathed new life into the notion of *lifelogging*, or the indiscriminate capture of life events and information³ in visual, auditory, and textual digital records – these records, ostensibly recording the life of the *logger*, also an not incidentally capture the

DOI: 10.21552/edpl/2017/4/4

* Jacquelyn Burkell, PhD, Associate Professor, Faculty of Information and Media Studies, The University of Western Ontario, London, Ontario, Canada. Her research focuses on the interaction between users and information, with particular emphasis on the influence of cognition on information use. For correspondence: jburkell@uwo.ca.

1 See, eg. Jacob Morgan, ‘Privacy is completely and utterly dead, and we killed it’ *Forbes* (19 August 2014) <<https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#48ca5e0231a7>> accessed 7 December 2017.

2 Louis D Brandeis and Samuel D Warren, ‘The right to privacy’ (1890) 4(5) *Harvard law review* 193-220, 195.

3 See, eg. James Condliffe, ‘Why Snap’s Spectacles are Going to (Finally) Make Lifelogging Cool’ (26 September 2016) *MIT Technology Review* <<https://www.technologyreview.com/s/602465/why-snaps-spectacles-are-going-to-finally-make-life-logging-cool/>> accessed 7 December 2017.

activities of others interacting with, or in the vicinity of, the person for whom the record is created. And then there is the veritable tsumani of transactional data that is created as a result of our everyday on line actions and interactions: searches completed, links visited, advertisements clicked on, files downloaded... all linked to a specific actor, tagged, tracked, and archived for future reference.

The second issue is the integration of these data. The personal information that is collected and stored online is shared and integrated through a variety of mechanisms. Again, most obvious are the social media practices wherein information shared in a social media profile becomes part of a more social public record as part of an unspoken but widely understood social contract regarding the 'publicness' of online social spaces.⁴ Third-party authentication, especially the use of social network logins to access third-party applications, provides a technical and policy infrastructure that enables the sharing of social media information across platforms, and the integration of information collected through different applications and on different devices. Third-party advertisers collate information about user activities on multiple sites. Terms of service and privacy policies disclose the often extensive data sharing and indeed data *selling* practices of online service providers. These data sharing and integration practices have the potential to knit together individually trivial bits of personal information into a meaningful and very detailed whole that, taken together, reveals a great deal about an individual,⁵ and supports the inference of even more⁶.

Finally, we have the permanence of the digital record. There is, as Mayer-Shönberger pointed out in his book *Delete*,⁷ no natural 'forgetting' mechanism in digital memory. Our ability to store the data we collect is only increasing – new technologies are emerging that allow *terabytes* of data to be stored in a single cubic centimetre.⁸ What this means is that data can be collected, and retained, 'just in case'. It also means that every one of us carries an accumulating online record of the minutiae of our everyday lives – a 'digital double' that reflects the totality of our online (and increasingly integrated offline) existence.

Together, these three conditions – the range of information being collected, the integration of information across multiple sources, and the permanence of the digital record – undergird the need for the 'right to be forgotten'. The digital record that follows each of us in our (online) lives threatens freedom, autonomy, and even identity⁹, limiting our capacity to define ourselves and live the lives we choose to live. The information

4 Jacquelyn Burkell et al, 'Facebook: Public space, or private space?' (2014) 17(8) *Information, Communication & Society* 974-985.

5 Jacquelyn Burkell, 'Remembering me: big data, individual identity, and the psychological necessity of forgetting' (2016) 18(1) *Ethics and Information Technology* 17-23.

6 Michal Kosinski, David Stillwell and Thore Graepel, 'Private traits and attributes are predictable from digital records of human behavior' (2013) 110(15) *Proceedings of the National Academy of Sciences* 5802-5805.

7 Viktor Mayer-Schönberger, *Delete: The virtue of forgetting in the digital age* (Princeton University Press 2011).

8 Liam Tung, 'This tiny storage breakthrough could hold 10 terabytes of data in one square centimetre' (*ZDnet*, 19 July 2016) <<http://www.zdnet.com/article/this-tiny-storage-breakthrough-could-hold-10-terabytes-of-data-in-one-square-centimetre/>> accessed 7 December 2017.

9 Burkell (n 5).

that is collected and remembered about each one of us is used to shape and even constrain the information we access, the advertisements we see, and even the prices that we pay. Patterns of past behaviour can be used to predict future actions; revealed personal information can be leveraged to identify other, unrevealed, aspects of the self. Protection against these data-driven incursions into our private lives requires that we maintain some control over what is known – and remembered – about us. We require, in other words, a right to be forgotten.

The ‘right to be forgotten’ presents practical difficulties with respect to development and enforcement, especially across international boundaries.¹⁰ In defining and implementing such a right, we can and will struggle with what it means to be forgotten, with how we would (and will) enforce a right to be forgotten, and with respect to what information (and under what circumstances) forgetting can be enforced. I would argue, however, that these struggles are *not* evidence of fatal flaws in the concept of the ‘right to be forgotten’; instead, I see these struggles as integral to the future of privacy, which is fundamentally threatened by the *lack* of forgetting that we now face.

Warren and Brandeis began their famous article, and their work of refining the legal protections for privacy, with this statement:

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.¹¹

I will close this foreword with the same, noting that we find ourselves in one of those critical times to which Warren and Brandeis refer, faced with the task of ‘defining anew’ the nature and extent of privacy protection – and particularly the nature and extent of the right to be forgotten – in light of technological and social changes that demand our attention.

¹⁰ See, eg, Steven C Bennett, ‘The right to be forgotten: Reconciling EU and US perspectives’ (2012) 30 Berkeley J Int’l L 161.

¹¹ Warren and Brandeis (n 2) 194.